Properties of improved ROPUF for FPGA generating multiple output bits from each pair of ROs

Filip Kodýtek, Róbert Lórencz and Jiří Buček

Czech Technical University in Prague
Faculty of Information Technology

CryptArchi, Leuven, 2015

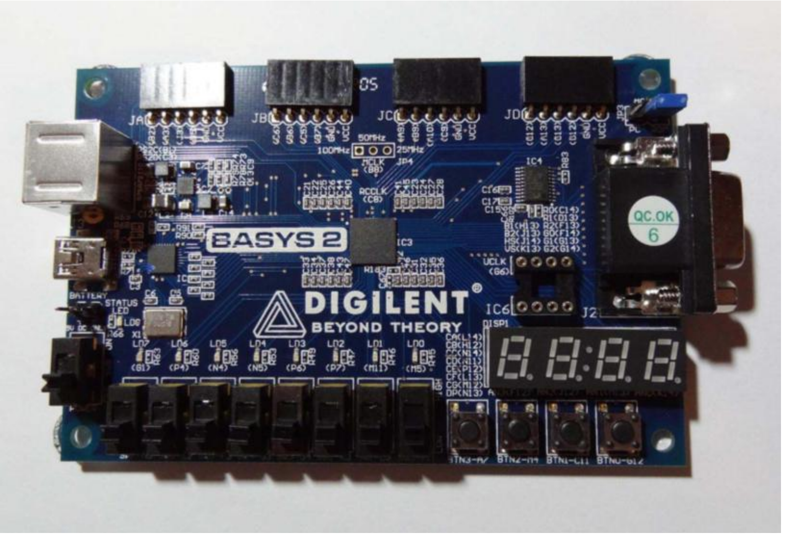
Outline

- Recapitulation of the ROPUF from CryptArchi 2014
- Gray code
- ROPUF Digilent Nexys 3
- Influence of voltage
- Timing analysis
- Conclusion

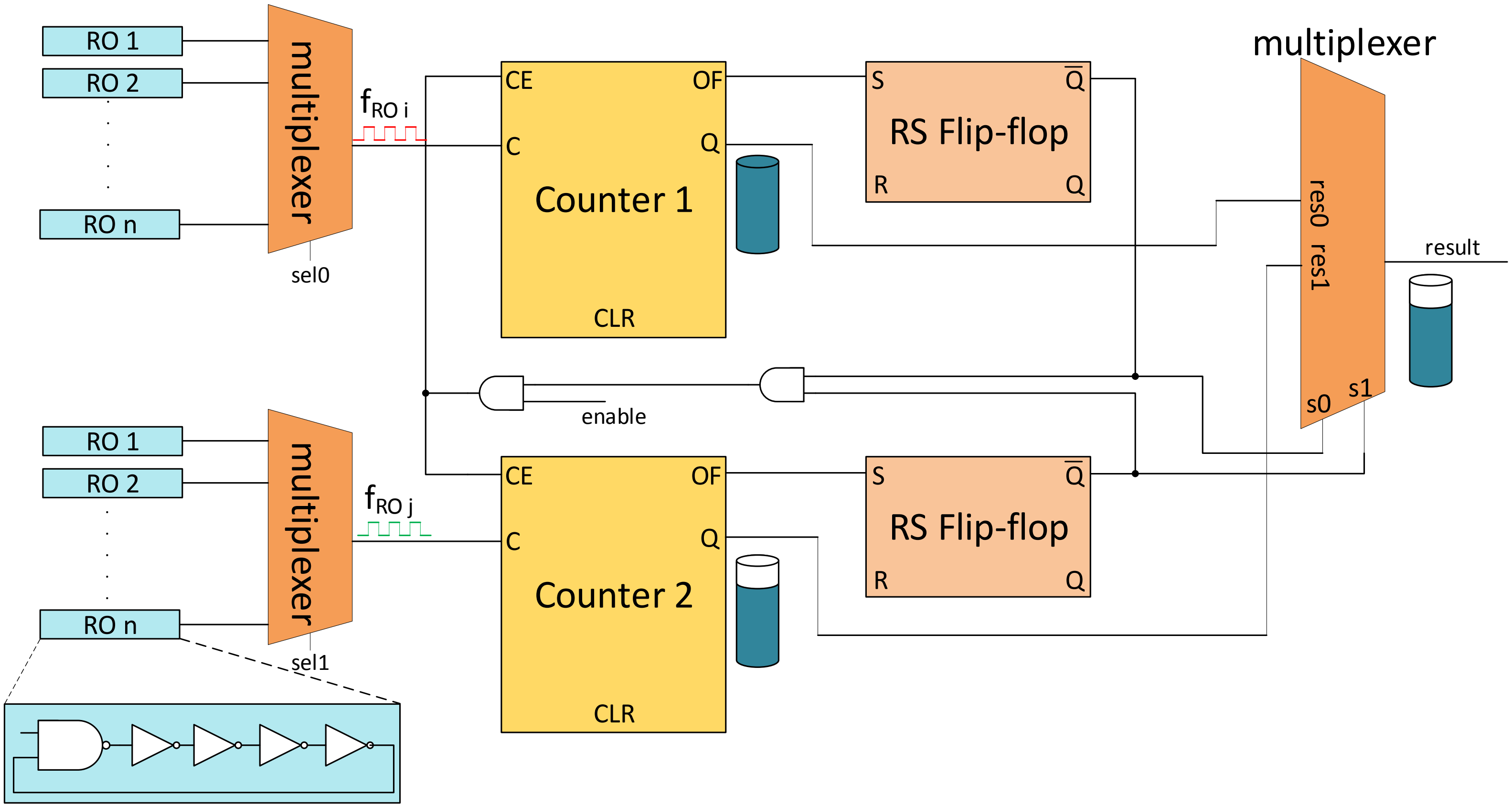
The proposed PUF

- Ring oscillator based PUF
  - The PUF output is generated from RO pairs
  - ROs **do not need** to be mutually **symmetric**
  - **More output bits** from each pair of ROs
    - obtained **from counter values**

- Statistical properties of the selected bits for PUF
  - Stability
  - Entropy
  - Bias
  - Hamming distance

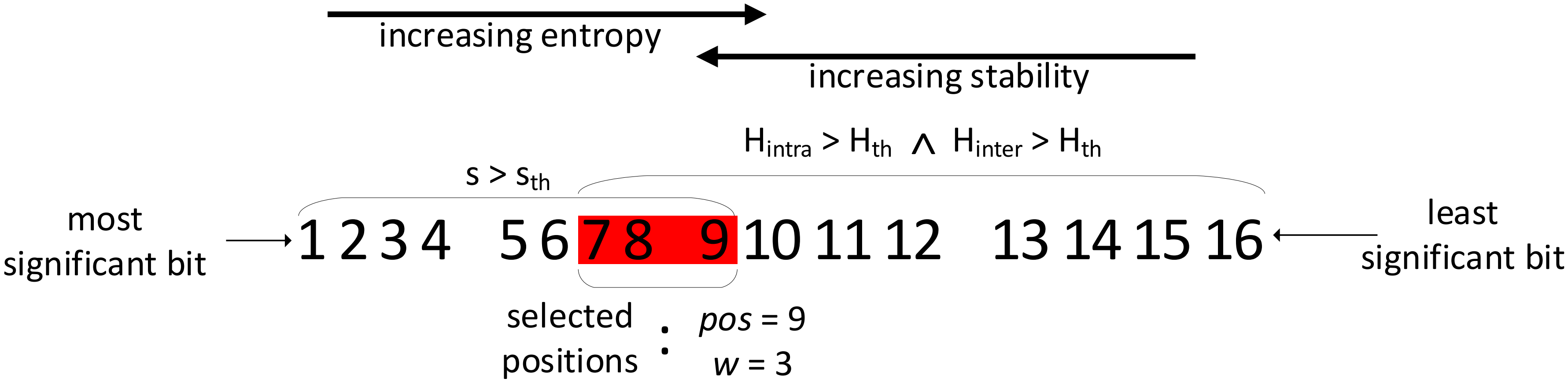


The circuit used for measurements



Processing the counter values

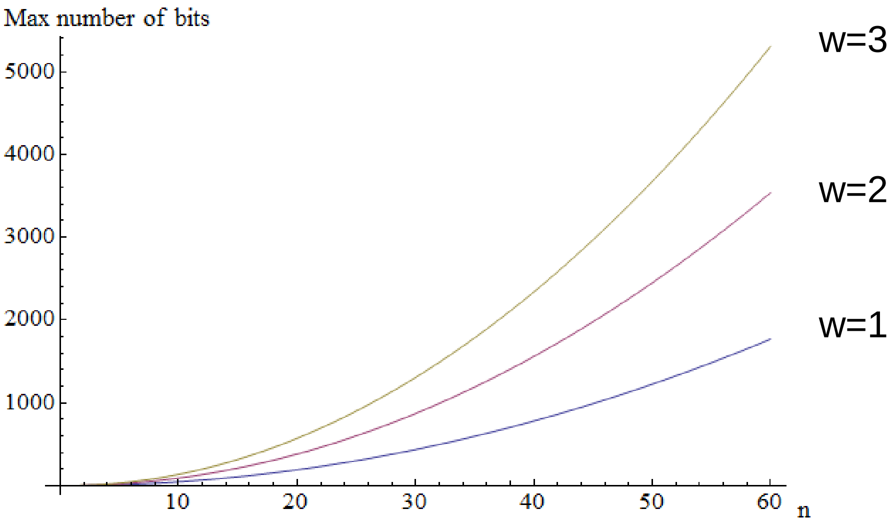
- Counter values represented in binary code
- Appropriately selected part of these values can be used directly for PUF – based on their entropy and stability
- We need to select positions, where both the entropy and stability are high
- s_{th} and H_{th} – threshold values of required stability and entropy



PUF design

- *w* bits from each RO pair
- Thus obtained bits are concatenated and form the PUF output
- Maximum amount of bits: $\binom{n}{2} * w$

$$\overbrace{10}^{RO_1}\overbrace{11}^{RO_2}\overbrace{01}^{RO_3}\ldots\overbrace{00}^{RO_{n-1}}\overbrace{10}^{RO_n}$$



Advantages:

- Area efficient
- Key generation

Position statistics

- Circuit with 300 ROs and 16-bit counters
- 450 RO pairs – 500 measurements
- ROs are not mutually symmetric
- Measurements performed on 24 Digilent Basys 2 FPGA boards (Xilinx Spartan3E-100 CP132)

	Position(i)	s_i	H_{intra}	H_{inter}	bias
MSB ↑	6	0.9961	0.9973	0.6585	0.5233
	7	0.9920	0.9982	0.9232	0.5118
	8	0.9841	0.9986	0.9682	0.4978
LSB ↓	9	0.9677	0.9984	0.9692	0.4971

Statistical evaluation of the PUF outputs

- Statistics for various selections of positions for 450 RO pairs
- BER and HD_{intra} should be ideally 0%
- Ideal value of HD_{inter} is 50%
- Green colour represents „almost ideal“

Positions	6-8	7-8	7-9	8-9
w	3	2	3	2
BER	0.92%	1.19%	1.87%	2.41%
HD_{intra}	1.37%	1.78%	2.79%	3.6%
HD_{intra} interval	<0%, 3.56%>	<0%, 4.56%>	<0.74%, 6.37%>	<1.11%, 8.22%>
HD_{inter}	42.69%	48.42%	48.94%	49.96%
HD_{inter} interval	<34.67%, 52.3%>	<42.33%, 56.11%>	<44.74%, 54.74%>	<45.44%, 54.67%>

Gray code

- Problem: overflow of particular part of the counter value when represented in binary code

Measurement 1: 1001 1111 1111 1111
Measurement 2: 1010 0000 0000 0000

- Can be solved by using Gray code

$$g_1 = b_1$$

$$g_i = b_i \oplus b_{i-1}$$

Binary	Gray
000	000
001	001
010	011
011	010
100	110
101	111
110	101
111	100

- The motivation to use Gray code is that only one bit changes when the value is incremented

Statistical evaluation of the PUF outputs with Gray code

- Results for 450 pairs of ROs
- We can select more bits with almost the same error rate

$$\overbrace{1011}^{RO_1}\overbrace{0100}^{RO_2}\ldots\overbrace{0010}^{RO_n}$$

Positions	7-8	7-9	7-10	8-9
w	2	3	4	2
BER	0.80%	1.08%	1.65%	1.62%
HD_{intra}	1.19%	1.60%	2.45%	2.40%
HD_{intra} interval	<0%, 2.78%>	<0.52%, 3.70%>	<0.78%, 5.33%>	<0.78%, 5.56%>
HD_{inter}	47.44%	48.3%	48.74%	49.97%
HD_{inter} interval	<35.89%, 60.33%>	<39.48%, 57.11%>	<41.61%, 56.39%>	<45.67%, 56.11%>

Statistical evaluation of the PUF outputs with Gray code

- 450 pairs of ROs
- Measurements performed on 6 Digilent Nexys 3 FPGA boards (Xilinx Spartan-6)
- Results are similar to Basys 2
- We can select the same positions as for Basys 2

(for example 7-10)

Positions	6-7	7-8	7-9	7-10
w	2	2	3	4
BER	0.53%	1.02%	1.31%	1.97%
HD$_{intra}$	0.81%	1.56%	1.98%	2.88%
HD$_{intra}$ interval	<0 %, 2%>	<0.33%, 3%>	<0.74%, 3.33%>	<1.28%, 4%>
HD$_{inter}$	40.27%	49.36%	49.3%	49.54%
HD$_{inter}$ interval	<28.67%, 55.67%>	<45.56%, 51.89%>	<47.33%, 51.26%>	<47.67%, 51.5%>

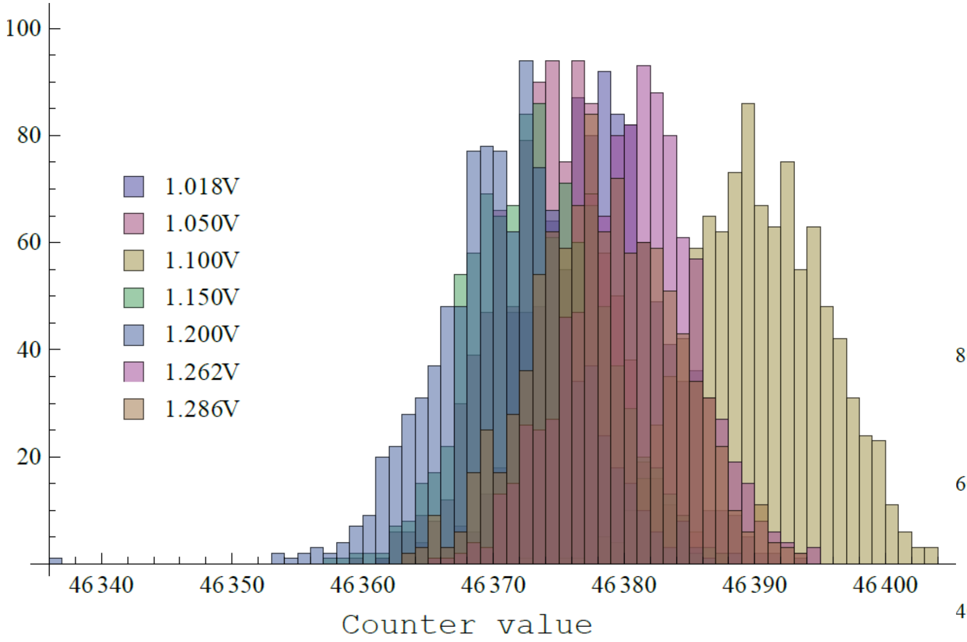
Influence of voltage

- Measurements performed on Digilent Basys 2 (Xilinx Spartan3E-100 CP132)
- The nominal voltage for power supply of the internal logic is 1.2V
- Recommended range from 1.14V to 1.26V
- Results for 150 RO pairs, positions 7-8

Voltage [V]	HD_{intra} [%]
1.200 → 1.018	49.00
1.200 → 1.050	51.67
1.200 → 1.100	54.33
1.200 → 1.150	34.00
1.200 → 1.262	44.00
1.200 → 1.286	49.00

Influence of voltage

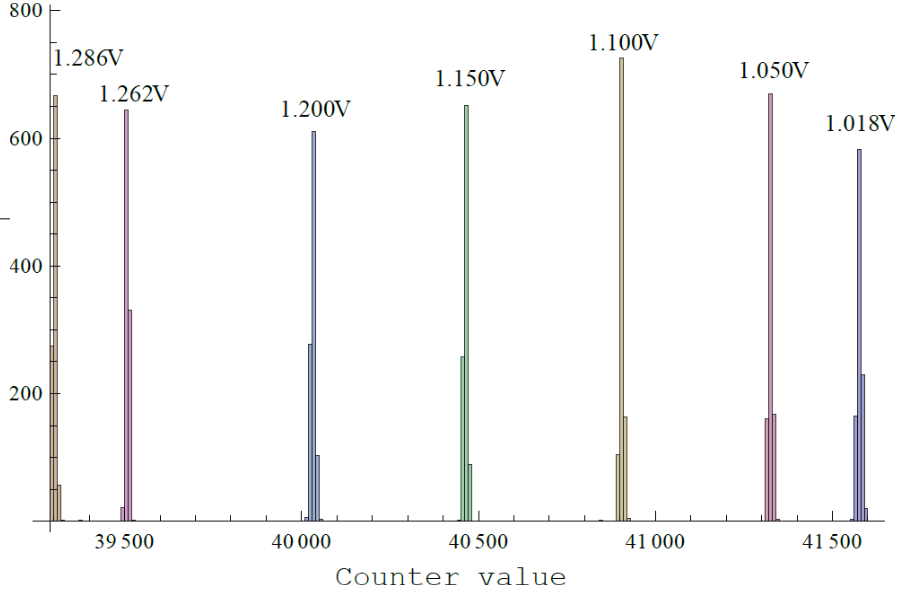
Desired behaviour



Dependence on:

- placement of ROs or
- selection of ROs or
- pairing of ROs?

Undesired behaviour



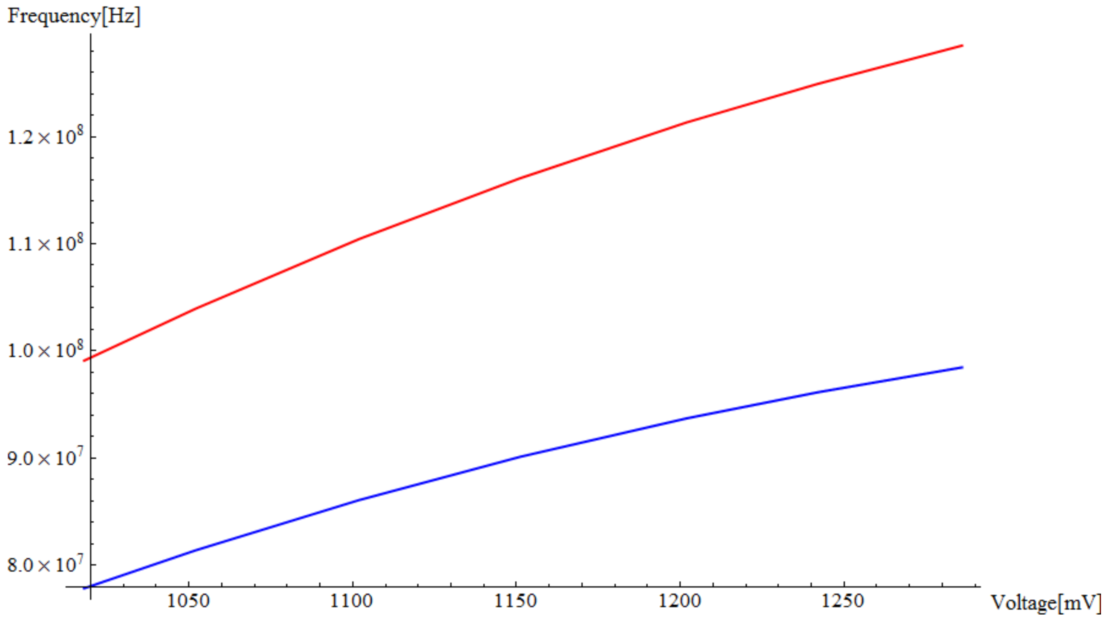
Will be studied in future work

Influence of voltage

- High sensitivity of this PUF design on voltage is caused by the change of ratios of 2 frequencies of ROs in each pair
- 16-bit counter value can be determined as:

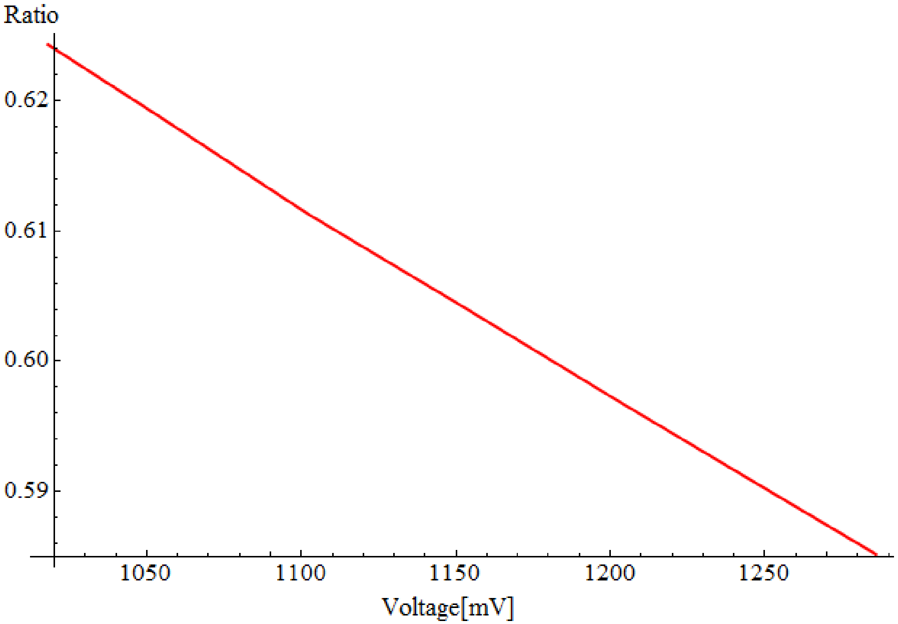
$$CounterValue = \frac{2^{16}}{f_1} * f_2$$

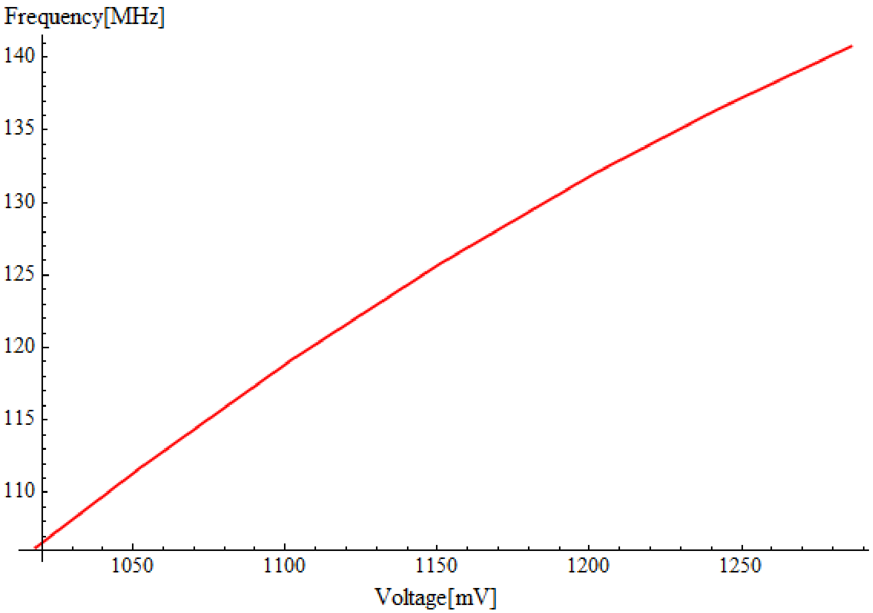
- f_1 is the frequency of the faster RO



Influence of voltage

- Measured ratio of frequencies for one RO pair





- Ideally, the ratio should be constant

Influence of voltage

- Measurements for voltages in the range from 1.180V to 1.222V (in recommended range)
- 150 RO pairs, positions 7-8

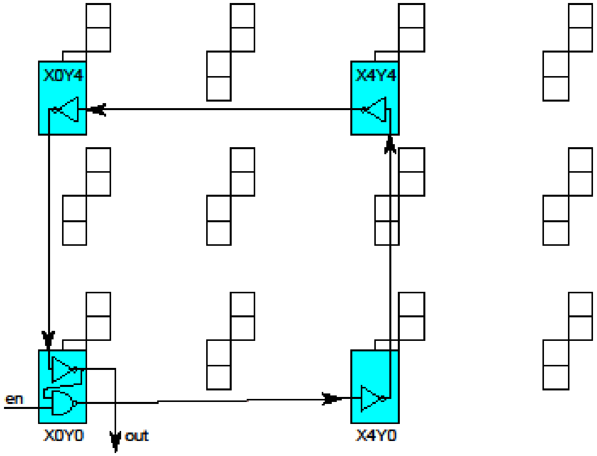
Voltage [V]	HD_{intra} [%]
1.201 → 1.180	19.67
1.201 → 1.190	9.00
1.201 → 1.193	7.33
1.201 → 1.196	5.33
1.201 → 1.207	4.33
1.201 → 1.212	8.33
1.201 → 1.222	18.00

- For HD_{intra} to be about 5%, the interval for voltage might be from 1.195V to 1.205V
- Similar results for 5-staged and 7-staged ROs

Placement of ROs

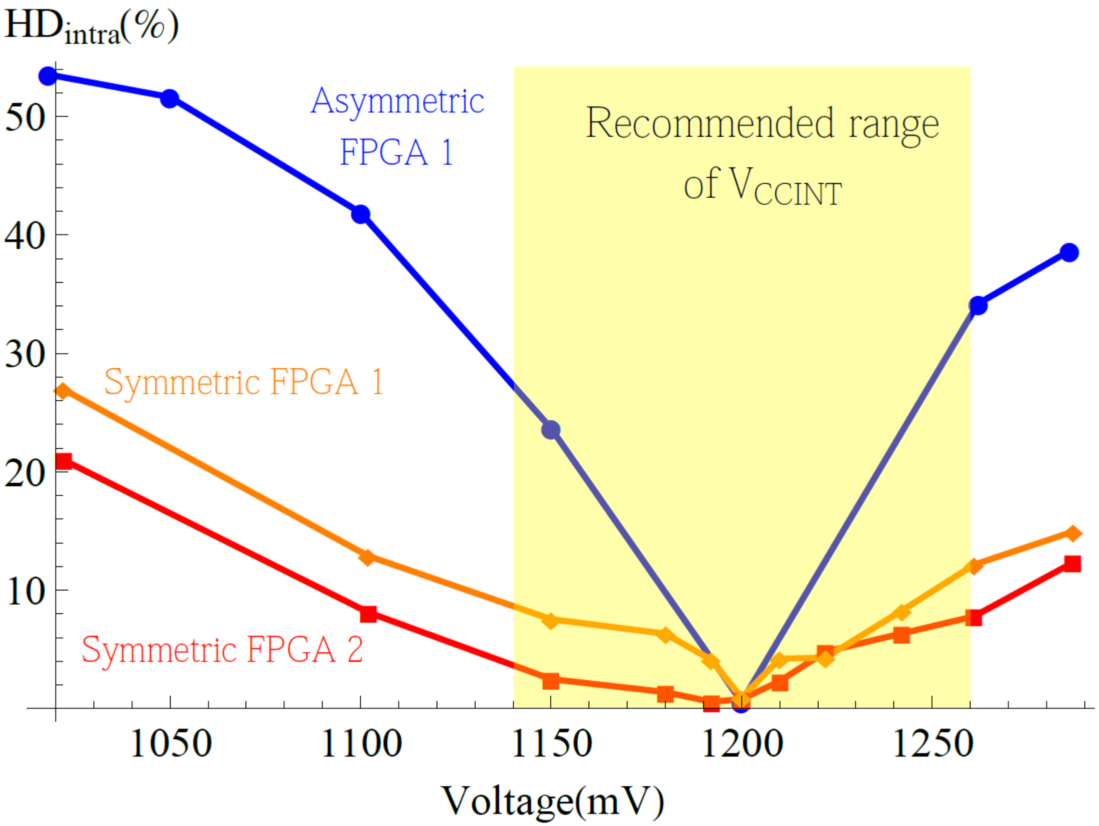
- Logic gates of ROs are placed so that the ROs are mutually symmetric
- 50 RO pairs, positions 7-8

	FPGA 1	FPGA 2
Voltage [V]	HD_{intra} [%]	HD_{intra} [%]
1.202 → 1.022	21.01	26.97
1.202 → 1.102	8.13	12.89
1.202 → 1.150	2.49	7.55
1.202 → 1.180	1.39	6.32
1.202 → 1.192	0.58	4.13
1.202 → 1.210	2.31	4.21
1.202 → 1.222	4.80	4.30
1.202 → 1.242	6.34	8.26
1.202 → 1.261	7.79	12.15
1.202 → 1.287	12.34	14.95



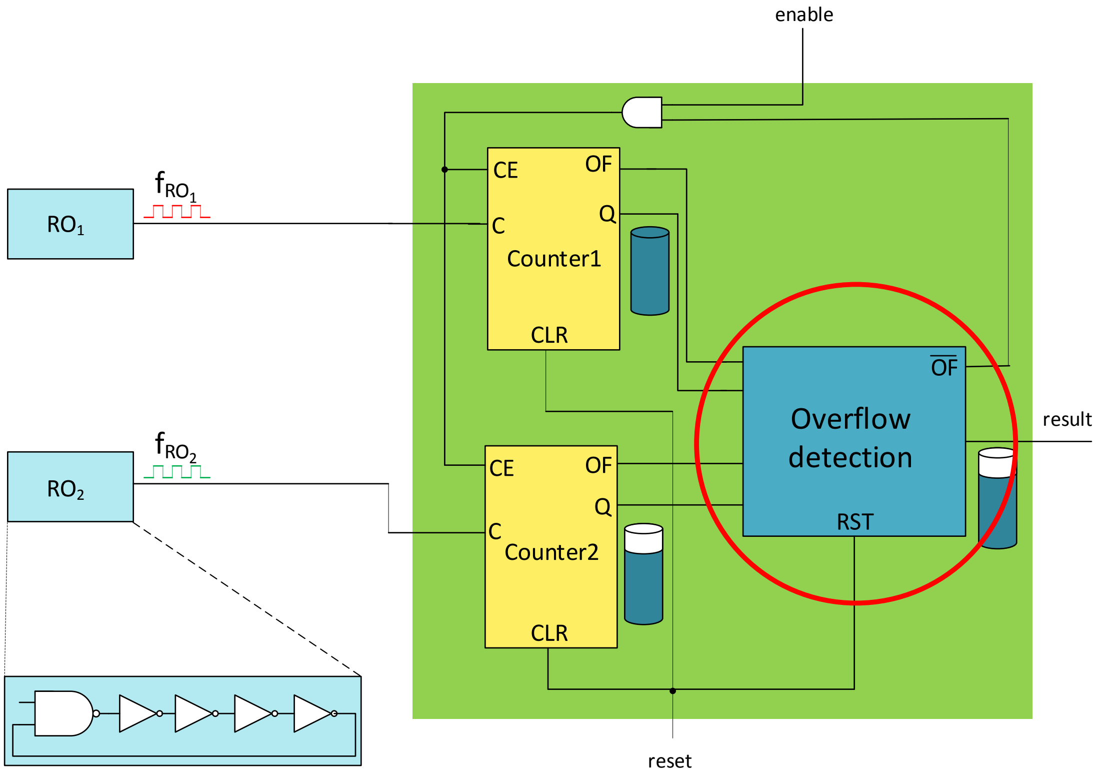
Placement of ROs

- Comparison of the behaviour of the proposed PUF when using mutually symmetric and asymmetric ROs for positions 7-8



Timing analysis

- To investigate the behaviour of ROs we performed more measurements using an oscilloscope
- We examined the impact of the delay of the circuit that detects the overflow and stops the measurement



Timing analysis

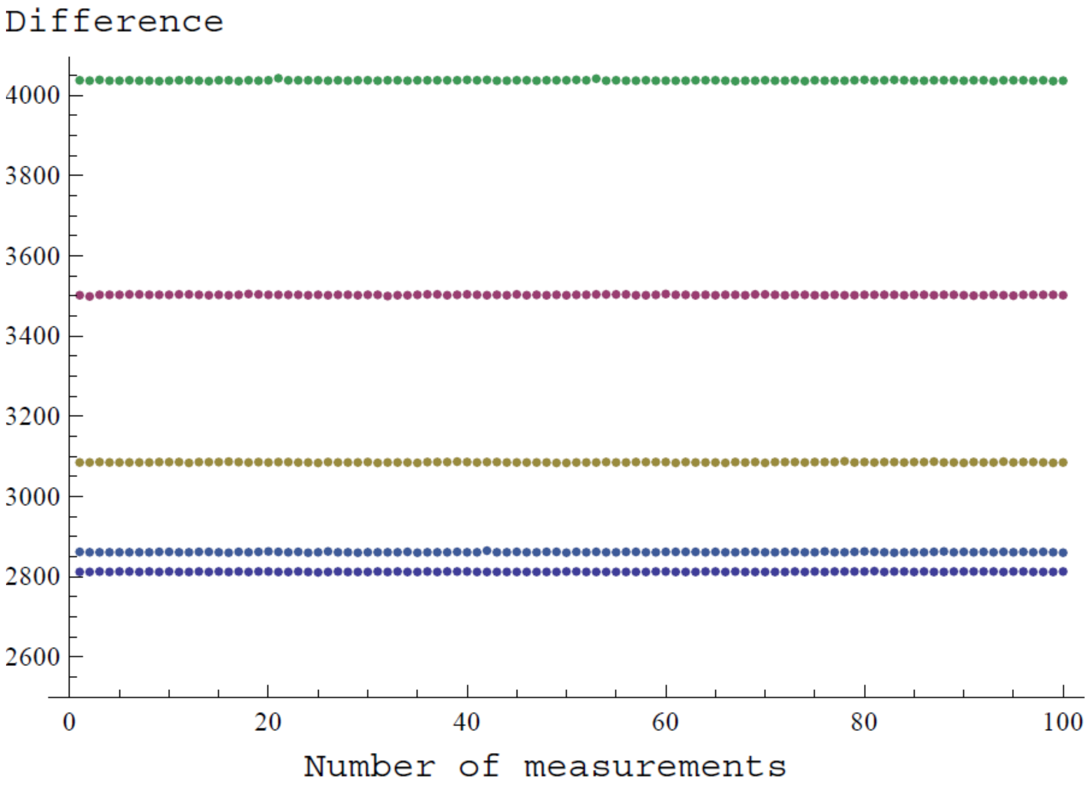
- By counting the rising edges of ROs, we determined the correct value that should be in the counter and compared it with the measured value

- The frequency of ROs may exceed the maximum operating frequency of the counters
  - Can be caused by variation in voltage or other reasons
  - Should be avoided by design
  - It causes the counters to miss some clock pulses
  - Even if this happens, the statistics for the PUF outputs remains the same

- When using fast enough counters, the difference of counter values to the correct ones should be ideally 0
  - The difference we measured was 0 or 1

Timing analysis

The difference of measured values with the correct ones when using „slow“ counters for 5 RO pairs



Conclusion

- We continued with the PUF design presented on CryptArchi 2014
- Gray code – more efficient PUF
- PUF design tested on Digilent Nexys 3 FPGA boards
- Influence of voltage
  - Strong dependence on voltage
  - Various properties for ROs
  - Analysis
- Verification of overflow detection circuit
- Independence on operating frequency of the counters

Thank you for your attention